



REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
UNITED STATES ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/
9th ARMY SIGNAL COMMAND
2530 CRYSTAL DRIVE
ARLINGTON, VA 22202

NETC-EST-SI

31 August 2005

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army-wide Common Access Card (CAC) Cryptographic Logon (CCL) Capability

1. References.

- a. Army Vice Chief of Staff Memorandum, subject: "Directives on Identity Protection Systems," 4 Aug 2005.
- b. Homeland Security Presidential Directive-12, 27 Aug 2004, subject: "Policy for a Common Identification Standard for Federal Employees and Contractors", 27 August 2004.
- c. DoD Instruction 8520.2, subject: "PKI and PK Enabling", 1 April 2004.
- d. Army CIO/G-6 Memorandum, subject: "Common Access Card (CAC) and Public Key Enabling (PKE)", 16 March 2004.
- e. DoD Directive 8190.3, subject: "Smart Card Technology", 31 August 2002.
- f. Army CIO/G-6 Message, subject: "Update for Implementation of PKI, CAC and PK-Enabling of Networks in the Department of the Army", 29 July 2002.

2. The Department of Defense (DoD) implemented Public Key Infrastructure (PKI) to support Defense-in-Depth strategies for increased information assurance and information systems protection. The CAC provides stronger authentication, data integrity, confidentiality, and technical non-repudiation of digital or electronic transactions. The Army has developed a capability to use a properly configured CAC to perform a CAC cryptographic logon (CCL) to the Army Enterprise (AE) and gain access to necessary resources.

3. A number of hurdles exist to using the CAC to logon to network resources. The first is the difficulty in obtaining timely, DoD Public Key Infrastructure (PKI) Certificate Validation (CV) information. The current DoD method of providing CV information (i.e., download the entire DoD certificate revocation list) does not provide an adequate solution. The Army is actively developing a viable CV solution that will support an enterprise-wide implementation of a CCL capability. A second is the completion of the Windows 2003/Active Directory (AD) network infrastructure required to support the CCL process. It is expected that AD will be deployed at most installations by Summer 2005 and fully deployed in time to support the beginning of CCL fielding currently scheduled for 1st Qtr FY06. The third is the requirement that the CAC used in the CCL process have the proper PKI certificates and a valid 6-8 digit PIN. Finally, all CCL users' workstations require a CAC/Smart Card reader and CAC middleware, both of which are widely implemented throughout the Army.

NETC-EST-SI

SUBJECT: Army-wide Common Access Card (CAC) Cryptographic Logon (CCL) Capability

4. The Army Office of Information Assurance and Compliance envisions a phased implementation for the CCL capability. The initial phase was completed during a CV operational assessment (OA) conducted at Fort Dix, NJ in Jan-Feb 05. The CCL capability was successfully implemented and demonstrated during the OA and is still in use. The second phase will consist of an initial fielding beginning in the 1st Qtr FY06. The last phase will be the Army wide fielding of CCL to be completed by 1st Qtr FY07.

5. To avoid delays with the CCL implementation, I request that the Director of Information Management (DOIM), in conjunction with the Garrison Military Personnel Directorate (GMPD) ensure that the following requirements are met:

a. Users must be migrated to AD


b. Each user's CAC must be configured with three Public Key Infrastructure (PKI) certificates (identity, email signature, and email encryption)

c. Users must know their 6-8 digit CAC PIN

d. User workstations must have Windows 2000 or Windows XP SP2 operating systems with a functioning CAC smart card readers and CAC middleware (ActivCard 3.0 or greater or NetSign 4.2 or greater).

6. Instructions to verify CAC and middleware requirements can be found at <https://iacapki.army.mil>. Users should be instructed to contact the local GMPD regarding CAC issues and the local DOIM for smart card and middleware issues.

7. POCs for this action are Mr. Kevin Watkins, commercial, (703)-602-7511, kevin.watkins@hqda.army.mil or Mr. Ken Lai, commercial, (703) 602-8346, ken.lai@us.army.mil.


COL, DEPUTY DIRECTOR
JOE C. CAPPS
Director
Enterprise Systems Technology Activity

DISTRIBUTION:

ASSISTANT SECRETARY OF ARMY (ACQUISITION, LOGISTICS AND TECHNOLOGY)
ASSISTANT SECRETARY OF THE ARMY (CIVIL WORKS)
(CONT)

NETC-EST-SI

SUBJECT: Army-wide Common Access Card (CAC) Cryptographic Logon (CCL) Capability

DISTRIBUTION: (CONT)

ASSISTANT SECRETARY OF THE ARMY (FINANCIAL MANAGEMENT AND
COMPTROLLER)

ASSISTANT SECRETARY OF THE ARMY (INSTALLATIONS AND ENVIRONMENT)

ASSISTANT SECRETARY OF THE ARMY (MANPOWER AND RESERVE AFFAIRS)

ADMINISTRATIVE ASSISTANT OF THE SECRETARY OF THE ARMY

THE INSPECTOR GENERAL

THE AUDITOR GENERAL

THE DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)

CHIEF OF LEGISLATIVE LIAISON

CHIEF OF PUBLIC AFFAIRS

DEPUTY CHIEF OF STAFF, G-1

DEPUTY CHIEF OF STAFF, G-2

DEPUTY CHIEF OF STAFF, G-3

DEPUTY CHIEF OF STAFF, G-4

DEPUTY CHIEF OF STAFF, G-8

ASSISTANT CHIEF OF STAFF FOR INSTALLATION MANAGEMENT

CHIEF OF ENGINEERS

THE SURGEON GENERAL

CHIEF, NATIONAL GUARD BUREAU

CHIEF, ARMY RESERVE

THE JUDGE ADVOCATE GENERAL

CHIEF OF CHAPLAINS

COMMANDER

U.S. ARMY EUROPE AND SEVENTH ARMY

EIGHTH U.S. ARMY

U.S. ARMY FORCES COMMAND

U.S. ARMY TRAINING AND DOCTRINE COMMAND

U.S. ARMY MATERIEL COMMAND

U.S. ARMY CORPS OF ENGINEERS

U.S. ARMY SPECIAL OPERATIONS COMMAND

U.S. ARMY PACIFIC

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

U.S. ARMY MILITARY TRAFFIC MANAGEMENT COMMAND

U.S. ARMY CRIMINAL INVESTIGATION COMMAND

U.S. ARMY MEDICAL COMMAND

U.S. ARMY MILITARY DISTRICT OF WASHINGTON

U.S. ARMY SOUTH

U.S. ARMY TEST AND EVALUATION

U.S. ARMY SAFETY CENTER

(CONT)

NETC-EST-SI

SUBJECT: Army-wide Common Access Card (CAC) Cryptographic Logon (CCL) Capability

DISTRIBUTION: (CONT)

U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND

COMMANDANT, U.S. MILITARY ACADEMY

PROGRAM EXECUTIVE OFFICER

AIR AND MISSILE DEFENSE

AMMUNITION

AVIATION

COMMAND, CONTROL, AND COMMUNICATIONS (TACTICAL)

CHEMICAL AND BIOLOGICAL DEFENSE

COMBAT SUPPORT AND COMBAT SERVICE SUPPORT

ENTERPRISE INFORMATION SYSTEMS

GROUND COMBAT SYSTEMS

INTELLIGENCE, ELECTRONIC WARFARE AND SENSORS

SOLDIER

SIMULATION, TRAINING AND INSTRUMENTATION

TACTICAL MISSILES

COMMANDER, U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH

ARMY SIGNAL COMMAND

NORTHEAST REGIONAL CHIEF INFORMATION OFFICE

NORTHWEST REGIONAL CHIEF INFORMATION OFFICE

SOUTHEAST REGIONAL CHIEF INFORMATION OFFICE

SOUTHWEST REGIONAL CHIEF INFORMATION OFFICE

PACIFIC REGIONAL CHIEF INFORMATION OFFICE

KOREA REGIONAL CHIEF INFORMATION OFFICE

EUROPE REGIONAL CHIEF INFORMATION OFFICE

CF:

DIRECTOR, INSTALLATION MANAGEMENT AGENCY